



INVESTOR IN PEOPLE

The Patent Office  
Concept House  
Cardiff Road  
Newport  
South Wales  
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation and Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein together with the Statement of inventorship and of right to grant of a Patent (Form 7/77), which was subsequently filed.

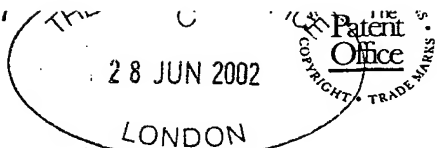
In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed


Dated 25 March 2003



# Statement of inventorship and of right to grant of a patent

The Patent Office

Cardiff Road  
Newport  
South Wales  
NP10 8QQ

1. Your reference	P014388GB RWP	
2. Patent number (if you know)	0215071.2	28 JUN 2002
3. Full name of the or of each applicant	SONY UNITED KINGDOM LIMITED	
4. Title of the invention	EMBEDDING DATA IN AN INFORMATION SIGNAL	
5. State how the applicant(s) derived the right from the inventor(s) to be granted a patent	BY VIRTUE OF AN ASSIGNMENT DATED 28 JUNE 2002.	
6. How many, if any, additional Patents Forms 7/77 are attached to this form? (see note (c))		
7.	<p>I/We believe that the person(s) named over the page (and on any extra copies of this form) is/are the inventor(s) of the invention which the above patent application relates to.</p> <p>Signature  Date 28 June 2002</p> <p>D Young &amp; Co (Agents for the Applicants)</p>	
8. Name and daytime telephone number of person to contact in the United Kingdom	Richard Pratt	023 8071 9500


## Notes

- a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.
- b) Write your answers in capital letters using black ink or you may type them.
- c) If there are more than three inventors, please write the names and addresses of the other inventors on the back of another Patents Form 7/77 and attach it to this form.
- d) When an application does not declare any priority, or declares priority from an earlier UK application, you must provide enough copies of this form so that the Patent Office can send one to each inventor who is not an applicant.
- e) Once you have filled in the form you must remember to sign and date it.

Patents Form 7/77

Patents Form 7/77

Enter the full names, addresses and postcodes of the inventors in the boxes and underline the surnames

Surname: <u>PELLY</u>	
First Names: Jason Charles	
2 Odell Close Lower Earley Reading Berkshire RG6 4DU United Kingdom	7972672001 
Patents ADP number (if you know it):	

Surname: _____	
First Names: _____	
Patents ADP number (if you know it):	

Surname: _____	
First Names: _____	
Patents ADP number (if you know it):	

Reminder

Have you signed the form?

# Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form 0

Description 13

Claim(s) 10

Abstract 1

Drawing(s) 5 + 5 Rm.

10. If you are also filing any of the following, state how many against each item.

Priority documents 0

Translations of priority documents 0

Statement of inventorship and right to grant of a patent (Patents Form 7/77) 2

Request for preliminary examination and search (Patents Form 9/77) 1

Request for substantive examination (Patents Form 10/77) 0

Any other documents (please specify) 0

11. I/We request the grant of a patent on the basis of this application.

Signature *D Young & Co* Date 28 June 2002  
D Young & Co (Agents for the Applicants)

12. Name and daytime telephone number of person to contact in the United Kingdom Richard Pratt 023 8071 9500

## Warning

*After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.*

## Notes

- If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.*
- Write your answers in capital letters using black ink or you may type them.*
- If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*
- If you have answered 'Yes' Patents Form 7/77 will need to be filed.*
- Once you have filled in the form you must remember to sign and date it.*
- For details of the fee and ways to pay please contact the Patent Office.*

28 JUN 2002

LONDON



01 JUL 02 15:27:00-1 00246  
P01/7700 0.00-0215071.2

## Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road  
Newport  
South Wales  
NP10 8QQ

1. Your reference

P014388GB RWP

2. Patent application number

(The Patent Office will fill in)

28 JUN 2002

3. Full name

(ear)

of the or of  
(all surnames)

SONY UNITED KINGDOM LIMITED  
THE HEIGHTS  
BROOKLANDS  
WEYBRIDGE  
KT13 0XW

Patents ADP number (if you know it)

If the applicant is a corporate body, give the country/state of its incorporation

UNITED KINGDOM

652270000 1

4. Title of the invention

EMBEDDING DATA IN AN INFORMATION SIGNAL

5. Name of your agent (if you have one)

D Young & Co

"Address for service" in the United Kingdom to which all correspondence should be sent (including the postcode)

21 New Fetter Lane  
London  
EC4A 1DA

Patents ADP number (if you know it)

59006

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and (if you know it) the or each application number.

Country

Priority application number  
(if you know it)

Date of filing  
(day / month / year)

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application

Date of filing  
(day / month / year)

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? (Answer 'Yes' if:

Yes

- a) any applicant named in part 3 is not an inventor, or
- b) there is an inventor who is not named as an applicant, or
- c) any named applicant is a corporate body.

See note (d))

Patents Form 1/77

Embedding Data in an Information Signal

BACKGROUND OF THE INVENTION

Field of the invention

The present invention relates to embedding data in an information signal.

- 5 Examples of the invention relate to: a method of and system for controlling copying of an information signal; an information signal; a data carrier on which an information signal is recorded; apparatus for modifying an information signal; a reproducing apparatus; and a computer program.

Description of the prior art

- 10 US-A-5,161,210 ( US Philips Corporation) discloses a system for inhibiting copying of audio signals. An audio signal is divided into frequency sub-bands and sub-band samples are quantized. The quantized samples are combined with samples of an auxiliary signal. The combined audio signal is recorded on a record carrier or transmitted. The auxiliary signal is inaudible in the combined audio signal. An audio  
15 signal reproducer having a recording unit also has a unit for detecting the auxiliary signal and generating a record control signal. The recording unit is constructed so that if a record control signal appears on its record control input the recording unit does not record the audio signal.

- WO 00/51348 (Macrovision) discloses a method and apparatus for inhibiting  
20 copying of audio or video signals transmitted over a cable television or direct satellite broadcast or the Internet. The signal is protected from unwanted copying by the combination of a watermark embedded in the signal at the head end together with additional copy protection data inserted in the signal. The additional data is a ticket. If the consumer pays a fee, the signal is transmitted to the consumer. The consumer can  
25 record only if the watermark and a mathematical function of the ticket match. The function is for example a hash function.

SUMMARY OF THE INVENTION

- According to one aspect of the present invention there is provided a method of controlling copying of an information signal in a system having a source of the  
30 information signal and a device for copying the information signal, the method comprising the steps of:

at an information signal modification source, prior to transmission of the information signal to the copying device, generating a copy control password and a related reference password, and applying to the information signal a substantially imperceptible modification representing copy control data including the copy control password securely encoded according to a predetermined algorithm;

delivering the modified information signal from the modification source to the copying device via a communications channel;

delivering the reference password from the modification source to the copying device via a separate communications channel independent of the modified information signal;

upon reception of the modified signal deriving the copy control data from the modified information signal;

comparing the derived securely encoded password with the separately provided reference password securely encoded according to a predetermined algorithm; and

enabling copying of the information signal if the securely encoded password derived from the information signal and the securely encoded reference password have a predetermined relationship.

Thus the present invention provides for conditional control of recording of an information signal instead of, or in addition to, simple denial of any recording and simple complete freedom to record or otherwise copy. Recording may be any form of storage including but not limited to storage on a linear data carrier, for example magnetic tape.

Furthermore, the reference password is not in the information signal or on any carrier of the information signal but is provided to the copying device independently of the information signal.

The information signal may represent any one of, or a combination of, image information (including still and moving images), audio, video, text, and data which may be executable or otherwise.

In examples of the invention the said copy control data includes other data indicating that copying is permitted subject to the provision by a user of a correct reference password.

The reference password is preferably securely encoded according to the same algorithm as the password derived from the information signal. The said predetermined algorithm may be an encryption algorithm. Preferably the said algorithm is a hash function in which case the reference password and the password  
5 derived from the information signal are the same. The reference password may be delivered to the copying device as a plain password or securely encoded, e.g. encrypted in which case it is decrypted at the copying device.

The reference password may be provided via a secure communications channel which is separate from the transmission channel of the information signal.

10 In an example of the invention, the reference password is provided to a user who wishes to copy the information signal. The password may be provided on a secure data carrier, e.g. a smart card or in some other, preferably secure, way. If provided on a smart card the reference password can be kept secure even from the user. The user provides the password to the copying device via an input device, e.g. a keyboard or a  
15 card reader. The user may be prompted to provide the password. Preferably that is done in response to the copy control data which indicates that copying is conditional upon the provision of the password. Thus the user is required to take positive action if they wish to copy an information signal for which copying is conditionally allowed.

A second aspect of the invention provides a method of applying copy control  
20 data to an information signal comprising the steps of:

determining whether copying of the information signal is allowed, not allowed or conditionally allowed; and

applying to the signal a substantially imperceptible modification representing copy control data, the copy control data comprising

- 25 a) first data if copying is allowed,  
b) second data if copying is not allowed, and  
c) third data if copying is conditionally allowed,

the third data including at least a password securely encoded according to a predetermined algorithm.

30 A third aspect of the invention provides a method of controlling the operation of a signal copying device having a recording unit controlled by a processor, the

copying device being operable to record an information signal produced by the method of the second aspect, the method comprising the steps of:

using the processor to derive the copy control data from the information signal and to determine whether the control data is the first, second or third data and to

5 a) allow the recording unit to record if the first data is present in the information signal,

b) disable the record unit if the second data is present in the information signal; and

10 c) allow the recording unit to record if the third data is present in the information signal and a reference password is provided which when securely encoded by a predetermined algorithm has a predetermined relationship to the said securely encoded password of the third data.

The second and third aspects of the present invention provide copy control data which explicitly indicates, and allows, conditional control of recording of an  
15 information signal and, in addition, simple denial of any recording and simple complete freedom to record.

It is possible that the copying device receives an information signal which does not have an imperceptible modification representing copy control data. In that case the copying device may be arranged to allow copying (or in the alternative not allow  
20 copying).

The copy control data may be used to control the copying device to operate in a predetermined manner. For example it may control the form of any copies for example indicating the form of copy control data to be included in any copy.

25 These and other aspects of the invention are set out in the accompanying claims.

### Brief description of the drawings

For a better understanding of the present invention, reference will now be made by way of example to the accompanying drawings in which:

Figure 1 is a schematic block diagram of an illustrative apparatus for applying  
5 a modification to an information signal in accordance with the invention;

Figure 2 is a schematic block diagram of an illustrative signal reproducing and recording apparatus in accordance with the invention;

Figures 3A and B are flow diagrams illustrating an operation performed by a processor of the apparatus of Figure 2;

10 Figure 4 is a schematic block diagram of an illustrative system for controlling copying in accordance with the invention;

Figure 5 is a schematic block diagram of an illustrative watermarking apparatus useful in the apparatus of Figure 1; and

15 Figure 6 is a schematic block diagram of an illustrative apparatus useful in the apparatus of Figure 2 for detecting a watermark and extracting data therefrom.

### Description of the Preferred Embodiments

Referring to Figure 1, a signal modifying apparatus 30 comprises a source 2 which produces an information signal which may be for example an audio signal, a video signal, an audio/video signal, a data signal and/or an image signals. The source 2  
20 may be any suitable source for example a signal reproducer which reproduces the signal from a record or an original source for example a camera in the case of video or microphone in the case of audio.

For ease of explanation the following description assumes the information signal is a video signal, but the invention is not limited to video.

25 A watermarking apparatus 6 receives the video signal from the source 2 and applies to it copy control data from a source 4. In this example the watermarking apparatus 6 embeds the copy control data in the video in such a way that the embedded data is substantially imperceptible in the video. Watermarking techniques are known in the art of video and an example of such a technique is described below with  
30 reference to Figure 5 but any other suitable known watermarking technique may be used.

The watermarking apparatus may optionally embed as a watermark provenance data, metadata, or other data in addition to the copy control data.

The copy control data is embedded for the purpose of controlling copying of the video signal. In one example of the invention, the data comprises a code  $h$  which is  
5 a hash function  $H(p)$  of a password  $p$ : i.e. the code  $h=H(p)$ . In another example of the invention, the control data  $h$  is associated with further data, for example 01 or 10, which indicates the presence of the code  $h$ .

In an example of the invention, the copy control data comprises a selected one of the following copy status codes:

- 10 00 which indicates no copying is allowed;
- 11 which indicates copying is freely allowed; and
- 01 or 10 together with code  $h$  which indicates that copying is allowed provided a reference password is provided which when hashed by the hash function  $H$  matches the code  $h$ .

15 The codes 00, 11 and 10 or 01 are examples of codes for simplicity of explanation. More complex codes may be used, Preferably codes which are unlikely to occur by chance are used.

The following description describes the currently preferred example but the invention is not limited to that example.

20 The video into which the control data is embedded by the watermarking apparatus 6 is fed to a recorder or transmitter 8. If fed to a recorder, the recorder 8 may record the watermarked video on a data carrier for example a disc or tape or semiconductor memory. If transmitted, the transmitter 8 may be for example a broadcast apparatus or a server which transmits the watermarked video to a  
25 distribution system.

Reference numeral 10 indicates a schematic representation of a distribution system which may be amongst other examples: an electronic communications network  
15 for transmitting the video e.g. a broadcast network, a PSTN or the Internet; or a physical distribution network via which tapes 13 or discs 11 or other data carriers on  
30 which the video is recorded are distributed.

The code source 4 also provides a reference password which in this example is the password  $p$ . The reference password  $p$  is fed via an interface 5 to a secure data

carrier, e.g. a smart card SC for delivery to a user of the video separately from the video. It will be appreciated that the reference password could be delivered by other means, e.g. another form of data carrier, on paper through the post or via the Internet or telephone system.

5           Figure 2 illustrates a copying device which in this example is a reproducing and recording apparatus 32. The apparatus 32 comprises a source 12 of video which may or may not be watermarked. The source 12 may reproduce the video from a data carrier or receive the video from a broadcast or other communications system as described above. The video is applied to a recording unit 22. The recording unit 22 is  
10           controlled by a record control signal produced by a control processor 14.

          Assume the video is watermarked.

          The control processor 14 comprises a watermark processor 16 which detects the watermark and derives the copy control data therefrom. Watermark processors capable of doing that are known and an example is described with reference to Figure  
15           6 below. A processor 18 decodes the copy control data and applies the appropriate record control signal to the recording unit. The control processor also has an input device 20 for entering the reference password. The input device may be a keyboard, smart card reader, an interface with an electronic communications channel, amongst other examples. In addition a display 17 may be provided. The display is used in an  
20           example of the invention to prompt the user to enter the reference password via the input device, for example by inserting the smart card SC into the input device 20.

          Referring to Figures 3A and B, the control processor 14 operates as follows:

          In step S1 the watermark processor 16 detects the watermark and derives the copy control data. In step S3 the processor 18 determines the value of the copy control  
25           data.

          If the copy control data is:

          00 then the record control signal is set S7 to disable the recording unit;

          11 then the record control signal is set S5 to enable recording by the recording unit; and

30           01 or 10 together with a code of any value then the user is requested S8 to provide a reference password p'.

Referring to Figure 3B, in step S81, the processor 18 detects whether the copy control data includes the code 01 or 10 indicating copying is allowed if the reference password is provided. If so, it causes a prompt to be displayed S82 by the display 17 requiring the user to enter the password.

5        If a reference password  $p'$  is entered S9 via an input device 20 the processor performs S11a hash function  $H(p')$  on the password and compares S13 the hashed reference password with the hash value  $h$  derived from the watermarked video. If the hashed values are the same S15 then copying is allowed S5. If the hashed values are not the same S15 then the recording unit is disabled S7.

10        If recording is enabled because the reference password is correct or because the copy control data = 11, then the watermarked video including the original copy control data is recorded to provide copy control of the copy.

The user of the reproducing apparatus 32 requires the reference password to copy video which has as copy control data the code 01 or 10 plus the hash value  $h$ . As  
15        will be described with reference to Figure 4, the reference password is supplied to the apparatus 32 separately from and independently of the watermarked video. In this example the password is provided on the smart card SC which is read by a card reader 20 which is the input device 20. This enables the password to be provided to a user and kept secret even from the user.

20        The smart card may be provided to a user on payment by the user of a fee.

The video from the source 12 may not have a copy control watermark. If the watermark processor 16 detects the absence of such a watermark, it indicates that to the processor 18; see step S1 of Figure 3A). The absence of the watermark may be regarded as either indicating copying is not allowed so that the processor outputs code  
25        00 to processor 18.. Currently it is preferred that the absence of the watermark indicates copying is allowed. Thus the processor 16 outputs code 11 to the processor 18.

The system of Figures 1 and 2 is illustrated by way of example as a special purpose system but could be implemented using programmable data processors.

30        In the system of Figure 4, the modifying apparatus 30 and the reproducing apparatus 32 are linked by communications interfaces I/F to a communications network 38 which is for example the Internet. There may be many reproducing

apparatus 321 to 32n connected to the network 38. For simplicity of description, it is assumed that the apparatus 30 is controlled by a seller and the user of the reproducing apparatus 32 is a buyer. Watermarked video is sent to buyers for example on a disc D via a distribution channel 10 for example a postal service or shop. If a buyer wishes to  
5 copy the watermarked video and it is watermarked with the copy control code 01 or 10 plus the hash value h, then the copy function in the reproducing apparatus 32 is disabled until the buyer pays a fee. The fee may be paid via the network 38 and a server 34, which for that purpose is linked to a financial institution 36, e.g. a credit card company.

10 The copy control hash values and/or the password may be unique to each user for increased security and traceability of unauthorised copies.

The payment of the fee is communicated to the seller via the network 38. The seller then releases the reference password for example on a smart card SC or in a secure manner via the communications network 38. Alternatively, the server may  
15 release the reference password on a smart card or via the network 38. For that purpose the server may communicate with the seller to obtain the reference password. It will be appreciated that the reference password could be delivered by other means, e.g. on a data carrier, on paper through the post or via the Internet or telephone system. Preferably the reference password is encrypted before transmission to the copying  
20 device 32 in which case it is decrypted at the copying device. Any known encryption system may be used.

The present invention assumes that all reproducing and recording apparatus are equipped with watermark detection and decoding apparatus which disables the recording unit of the apparatus.

25 Watermarking, Figure 5

Figure 5 illustrates the watermarking apparatus denoted as embedder 120 in more detail. The watermark embedder 120 comprises pseudo-random sequence generator 220, an error correction coding generator 200, a wavelet transformer 210, an inverse wavelet transformer 250, a first combiner 230, a data converter 225 and a  
30 second combiner 240. The wavelet transformer 210 includes a frame store FS1. The inverse transformer 250 includes a frame store FS2. The frame store FS1 stores a

frame of unmodified coefficients  $C_i$ . The frame store FS2 stores a frame of modified coefficients  $C_i'$ .

The error correction coding generator 200 receives the copy control data and outputs an error correction coded copy control data to the first combiner 230. The pseudo-random sequence generator 220 outputs a pseudo-random binary sequence (PRBS)  $P_i$ , where  $i$  is the  $i^{\text{th}}$  bit of the sequence, to the first combiner 230. The PRBS has a length  $L \times J$  of bits where  $J$  is the number of bits in the error correction encoded copy control data. Each bit  $j$  of the error correction encoded copy control data then modulates a section of length  $L$  of the PRBS. The first combiner 230 logically combines the error correction encoded copy control data with the PRBS to produce a watermark having bits  $R_i$ . A bit  $W_j=0$  of the error correction encoded copy control data inverts  $L$  bits of the PRBS. A bit  $W_j=1$  of the error correction encoded copy control data does not invert the PRBS. Thus bits  $W_j$  of the error correction encoded copy control data are spread over  $L$  bits of the PRBS. The data converter 225 converts binary 1 to symbol  $+1$  and binary 0 to symbol  $-1$  to ensure that binary 0 bits contribute to a correlation value used in the decoder of Figure 5.

The wavelet transformer 210 receives the video image  $I$  from the source 110 and outputs wavelet coefficients  $C_i$  to the second combiner 240.

The second combiner 240 receives the watermark  $R_i$ , the wavelet coefficients  $C_i$  and watermark strength  $\alpha_i$  and outputs modified coefficients  $C_i'$  where

$$C_i' = C_i + \alpha_i R_i$$

The inverse wavelet transformer 250 receives the modified coefficients  $C_i'$  and outputs a spatial domain watermarked image  $I'$ .

The embedder includes an ECC generator 200. The use of error correction coding to produce an error correction coded copy control data is advantageous since it allows the copy control data 175 to be reconstructed more readily should some information be lost. This provides a degree of robustness to future processing or attacks against the watermark. The use of a pseudo-random sequence  $P_i$  to generate a spread spectrum signal for use as a watermark is advantageous since it allows the error correction coded copy control data 205 to be spread across a large number of bits. Also, it allows the watermark to be more effectively hidden and reduces the visibility of the watermark. Applying the watermark to a wavelet transform of the image is

advantageous since this reduces the perceptibility of the watermark. Furthermore, the strength of the watermark is adjusted by  $\alpha_i$  to ensure that the watermark is not perceptible.

Detecting copy control data in watermarked video, Figure 6

5 The operation of the watermark processor denoted as decoder 140 will now be explained in more detail with reference to Figure 6. The watermark decoder 140 receives the watermarked image  $I'$  and outputs the restored copy control data. The watermark decoder 140 comprises a wavelet transformer 310, a reference pseudo-random sequence (PRBS) generator 320, a correlator 330, a selector 340 and a error  
10 correction coding decoder 350. The PRBS generated by the generator 320 is identical to that generated by the PRBS generator 220 of Figure 2 and converted by a data converter (not shown) to values +1 and -1 as described above.

The wavelet transformer 310 receives the watermarked image  $I'$  and, in known manner, outputs the modified wavelet coefficients  $C_i'$ . The correlator 330 receives the  
15 reference pseudo-random sequence PRBS having symbols  $P_i$  of values +1 and -1 from the pseudo-random sequence generator 320, and the wavelet coefficients  $C_i'$  and outputs a watermark image bit correlation sequence 335. The watermarked image bit correlation sequence is determined in the following way.

The modified wavelet coefficients  $C_i' = C_i + \alpha_i R_i$  where  $R_i$  are bits of PRBS  
20 modulated by error-correction encoded bits  $W_j$  of copy control data. Each bit  $W_j$  modulates  $L$  bits of PRBS. There are  $JL$  bits in the modulated PRBS. For each error correction encoded bit  $W_j$ , the correlator 330 calculates a correlation value

$$S_j' = \sum_{i=jL+1}^{jL+L} C_i' \cdot P_i$$

25 where  $j = 0, 1, 2, \dots, J-1$ , and  $J$  is the number of error correction encoded bits. A sequence 335 of correlation values  $S_j'$  is produced.

The correlation sequence 335 is received by the selector 340 which outputs an uncorrected copy control data 345. The selector 340 outputs a bit value "1" for a value of  $S_j'$  greater than 0 and a bit value "0" for  $S_j'$  less than or equal to 0. The error

correction code decoder 350 receives the uncorrected copy control data 345 and in known manner outputs the restored copy control data 145.

The reference PRBS Pi is synchronised with the modulated PRBS in the watermarked image. For that purpose a synchroniser (not shown) is used. Such  
5 synchronisation is known in the art.

#### Modifications

Although Figures 5 and 6 give an example of watermarking using Wavelet coefficients, the invention is not limited to Wavelets but can be implemented using other watermarking techniques including the use of DCT coefficients.

10 Although the invention has been illustrated by reference to Figures 1 to 4 which show schematics of special purpose hardware, it is envisaged that the invention may be implemented in software on programmable machines. Thus the invention also encompasses software which when run on suitable data processing equipment implements the functions described herein.

15 The information signal whether stored on a data carrier or sent as a signal via a communications channel may include several parts representing different sections of content or different items of content. For example a disc or tape typically has several tracks. In an embodiment of the invention each section may have its own copy control data embedded as an imperceptible watermark each with its own copy status and/or its  
20 own password. For example if a disc has tracks one to four the copy control data may be as follows:

Track	Copy Status Data	Password
Track 1	00	-
Track 2	01	nnnnnn
Track 3	01	mmmm
Track 4	11	-

Thus track 1 can be copied freely. Track 2 may be copied if the password nnnnnn is provided. Track 3 may be copied if password mmmmm is provided, Copying  
25 of track five is not allowed. A user may be provided with only one of the passwords.

In a further embodiment, the copy status codes define copying rights for a user in addition to copying allowed, not allowed and conditionally allowed. For example

code 01( plus the password) may indicate copying is conditionally allowed but the copies retain the original copy control data signifying the conditional copying status whereas code 10 may indicate copying is conditionally allowed and the copy may be freely copied, the copy control data not being retained in the first copy. Code 10 may  
5 be used to protect content whilst in transit between a supplier and the user for example.

Other status codes with passwords forming the copy control data may indicate other copying status.

In embodiments in which the copy status data is changed, the watermark must be amendable. Watermarks which may be removed are described in for example co-  
10 pending European patent application 1215880.. The processors 16 and 18 in the control processor 14 of Figure 2 are arranged to remove the original watermark and replace it with a new one. The new one may be permanent or removable.

CLAIMS

1. A method of controlling copying of an information signal in a system having a source of the information signal and a device for copying the information signal, the method comprising the steps of:

5 at an information signal modification source, prior to transmission of the information signal to the copying device, generating a copy control password and a related reference password, and applying to the information signal a substantially imperceptible modification representing copy control data including the copy control password securely encoded according to a predetermined algorithm;

10 delivering the modified information signal from the modification source to the copying device via a communications channel;

delivering the reference password from the modification source to the copying device via a separate communications channel independent of the modified information signal;

15 upon reception of the modified signal deriving the copy control data from the modified information signal;

comparing the derived securely encoded password with the separately provided reference password securely encoded according to a predetermined algorithm; and

20 enabling copying of the information signal if the securely encoded password derived from the information signal and the securely encoded reference password have a predetermined relationship.

2. A method according to claim 1, wherein the reference password is securely encoded according to the same algorithm as the derived password.

25

3. A method according to claim 1 or 2, wherein the copy control data additionally includes other data indicating that copying is permitted if a correct reference password is provided.

4. A method according to claim 1, 2 or 3, wherein the copy control password and the reference password are the same and the predetermined algorithm is a hash function.

5 5. A method according to claim 1, 2, 3 or 4, wherein the reference password is delivered to the copying device by the steps of providing the reference password to a user of the information signal who provides the reference password to the copying device.

10 6. A method according to claim 5, wherein the reference password is provided to the user if the user fulfils at least one predetermined condition.

7. A method according to claim 6, wherein the condition is payment for provision of the password.

15

8. A method according to claim 5, 6 or 7 wherein the password is provided to the user via a secure communications channel.

9. A method according to claim 5, 6 or 7 wherein the password is  
20 provided to the user on a secure data carrier.

10. A method according to any preceding claim, comprising the step of prompting the user to provide the password, the prompting of the user occurring in response to the derivation of the copy control data.

25

11. A method according to any preceding claim, comprising the step of storing the modified information signal on a data carrier for supply to the said user.

12. A method according to any preceding claim wherein the modification is  
30 applied to the information signal by modifying transform coefficients of the information signal.

13. A method according to claim 12, wherein the said coefficients are DCT or Wavelet coefficients.

14. A method according to any preceding claim, wherein the information  
5 signal comprises any one or more of: image information, video information, audio information, text and data.

15. A system for controlling copying of an information signal the system having a source of the information signal and a device for copying the information  
10 signal and further comprising:

an information signal modification apparatus operable, prior to transmission of the information signal to the copying device, to generate a copy control password and a related reference password, and apply to the information signal a substantially imperceptible modification representing copy control data including the copy control  
15 password securely encoded according to a predetermined algorithm;

a communications channel for delivering the modified information signal from the modification source to the copying device; and

a separate communications channel independent of the modified information signal for delivering the reference password from the modification source to the  
20 copying device; wherein

the copying device comprises a data processor and an input device for providing the reference password to the data processor, the data processor being operable to

a) derive the copy control data from the modified information signal upon  
25 reception of the modified signal, and

b) compare the derived securely encoded password with the separately provided reference password securely encoded according to a predetermined algorithm; and

c) a copying unit enabled by the data processor to copy the information signal  
30 if the securely encoded password derived from the information signal and the securely encoded reference password have a predetermined relationship.

16. A system according to claim 15, wherein the data processor is arranged to securely encode the reference password according to the same algorithm as the derived password.

5 17. A system according to claim 15, or 16, wherein the predetermined algorithm is a hash function.

18. A system according to claim 15, 16 or 17, wherein the input device is a keyboard.

10

19. A system according to claim 15, 16 or 17, wherein the input device is a reader for reading data from a data carrier.

20. A system according to claim 15, 16 or 17, wherein the input device  
15 comprises a communications interface for receiving the reference password from a communications network.

21. A system according to any one of claims 15 to 20, wherein the signal  
20 modification apparatus is operable to apply the modification by modifying transform coefficients of the information signal.

22. A system according to claim 21, wherein the transform coefficients are DCT or Wavelet coefficients.

25 23. A system according to any one of claims 15 to 22, further comprising means for prompting a user to provide the reference password to the data processor via the input device.

24. An information signal to which is applied a substantially imperceptible  
30 modification representing copy control data including a password securely encoded according to a predetermined algorithm and other data indicating that copying is permitted if a correct reference password is provided.

25. A signal according to claim 24, wherein the predetermined algorithm is a hash function.

5        26. A signal according to claim 24 or 25, wherein the modification is applied to the information signal by modifying transform coefficients of the information signal.

27. A signal according to claim 26, wherein the said coefficients are DCT  
10 or Wavelet coefficients.

28. A signal according to any one of claims 24 to 27, which comprises any one or more of image information, video information, audio information, text and data.

15        29. A data carrier on which is recorded a signal according to any one of claims 24 to 28.

30. A data carrier according to claim 29 which is a disc.

20        31. A signal modification apparatus operable to apply to an information signal a substantially imperceptible modification by modifying transform coefficients of the information signal, the modification representing copy control data including a password securely encoded according to a predetermined algorithm and other data indicating that copying is permitted if a correct reference password is provided.

25

32. Apparatus according to claim 31, wherein the predetermined algorithm is a hash function.

33. Apparatus according to claim 31 or 32, wherein the said coefficients are  
30 DCT or Wavelet coefficients.

34. An information signal copying device for copying an information signal to which is applied a substantially imperceptible modification representing copy control data including a password securely encoded according to a predetermined algorithm, the copying device comprising:

5 a data processor operable to receive the modified information signal, and an input device for receiving a reference password separately from, and independently of, the modified information signal, and for providing the reference password to the data processor,

the data processor being operable to

10 a) derive the copy control data from the modified information signal upon reception of the modified signal, and

b) compare the derived securely encoded password with the separately provided reference password securely encoded according to a predetermined algorithm; and

15 c) a copying unit enabled by the data processor to copy the information signal if the securely encoded password derived from the information signal and the securely encoded reference password have a predetermined relationship.

35. A processing apparatus according to claim 34, wherein the data  
20 processor is arranged to securely encode the reference password according to the same algorithm as the derived password.

36. A processing apparatus according to claim 33 or 34, wherein the  
predetermined algorithm is a hash function.

25

37. A processing apparatus according to claim 34, 35 or 36, wherein the input device is a keyboard.

38. A processing apparatus according to claim 34, 35 or 36, wherein the  
30 input device is a reader for reading data from a data carrier.

39. A processing apparatus according to claim 34, 35 or 36, wherein the input device comprises a communications interface for receiving the reference password from a communications network.

5           40. A processing apparatus according to any one of claims 34 to 39 further comprising means for prompting a user to provide the reference password via the input device.

41. A method of applying copy control data to an information signal  
10 comprising the steps of:

determining whether copying of the information signal is allowed, not allowed or conditionally allowed; and

applying to the signal a substantially imperceptible modification representing copy control data, the copy control data comprising a copy status code of

15           a) first data if copying is allowed,  
            b) second data if copying is not allowed, and  
            c) third data if copying is conditionally allowed,

the third data including at least a password securely encoded according to a predetermined algorithm.

20           42. A method according to claim 41, wherein the third data also includes other data indicating that copying is allowed on provision of a reference password.

43. A method according to claim 41 or 42, wherein the predetermined  
25 algorithm is a hash function.

44. A method according to claim 41, 42 or 43, wherein the modification is applied to the information signal by modifying transform coefficients of the information signal.

30           45. A method according to claim 44, wherein the said coefficients are DCT or Wavelet coefficients.

46. A method according to any one of claims 41 to 45, wherein the information signal comprises any one or more of: image information, video information, audio information, text and data.

5

47. A method of controlling the operation of a signal copying device having a recording unit controlled by a processor, the copying device being operable to record an information signal produced by the method of any one of claims 41 to 46, the method comprising the steps of:

10 using the processor to derive the copy control data from the information signal and to determine whether the control data is the first, second or third data and to

a) allow the recording unit to record if the first data is present in the information signal,

15 b) disable the recording unit if the second data is present in the information signal; and

c) allow the recording unit to record if the third data is present in the information signal and a reference password is provided which when securely encoded by a predetermined algorithm has a predetermined relationship to the said securely encoded password of the third data.

20

48. A method according to claim 47, comprising the step of securely encoding the reference password according to the same algorithm as the said password of the third data.

25

49. A method according to claim 48 wherein the algorithm is a hash function.

50. A method according to any one of claims 47 to 49, comprising the step of providing the reference password to the processor separately from the information  
30 signal.

51. A method according to claim 50, comprising the step of providing the reference password to the processor via a user.

52. A method according to claim 51, further comprising the step of  
5 prompting the user to provide the reference password.

53 A method according to claim 52, comprising the step of prompting the user to provide the password, the prompting of the user occurring in response to the derivation of the third data.

10

54. A method according to any one of claims 47 to 53, which includes using the said processor to detect whether or not a substantially imperceptible modification representing the copy control data is present in the information signal and, if it is not present, producing data which controls the recording unit in a  
15 predetermined manner.

55. A method according to claim 54, wherein the said processor produces the said first data allowing the recording unit to record if the copy control data is not present in the information signal.

20

56. A method according to any one of claims 47 to 55 of recording an information signal according to claim 42 wherein the third data indicates a copy may be made on provision of a reference password and the copy includes an imperceptible modification representing copy control data defined by the third data and comprising  
25 the step of applying to the copy an imperceptible modification representing copy control data defined by the third data..

57. A method according to claim 56, wherein the said modification applied to the copy is different from that of the original signal.

30

58. Apparatus arranged to carry out the method of one of claims 41 to 57.

59. A computer program which when run on a suitable processing system implements the method of one of claims 1 to 14 and 41 to 57.

60. A method of controlling copying substantially as hereinbefore  
5 described with reference to Figures 1 to 4 of the accompanying drawings.

61. A system for controlling copying substantially as hereinbefore described with reference to Figures 1 to 4 of the accompanying drawings.

10 62. Apparatus for applying copy control data to an information signal substantially as hereinbefore described with reference to Figure 1 optionally as modified by Figure 5 of the accompanying drawings.

15 63. Recording apparatus substantially as hereinbefore described with reference to Figures 2 and 3 optionally as modified by Figure 6 of the accompanying drawings.

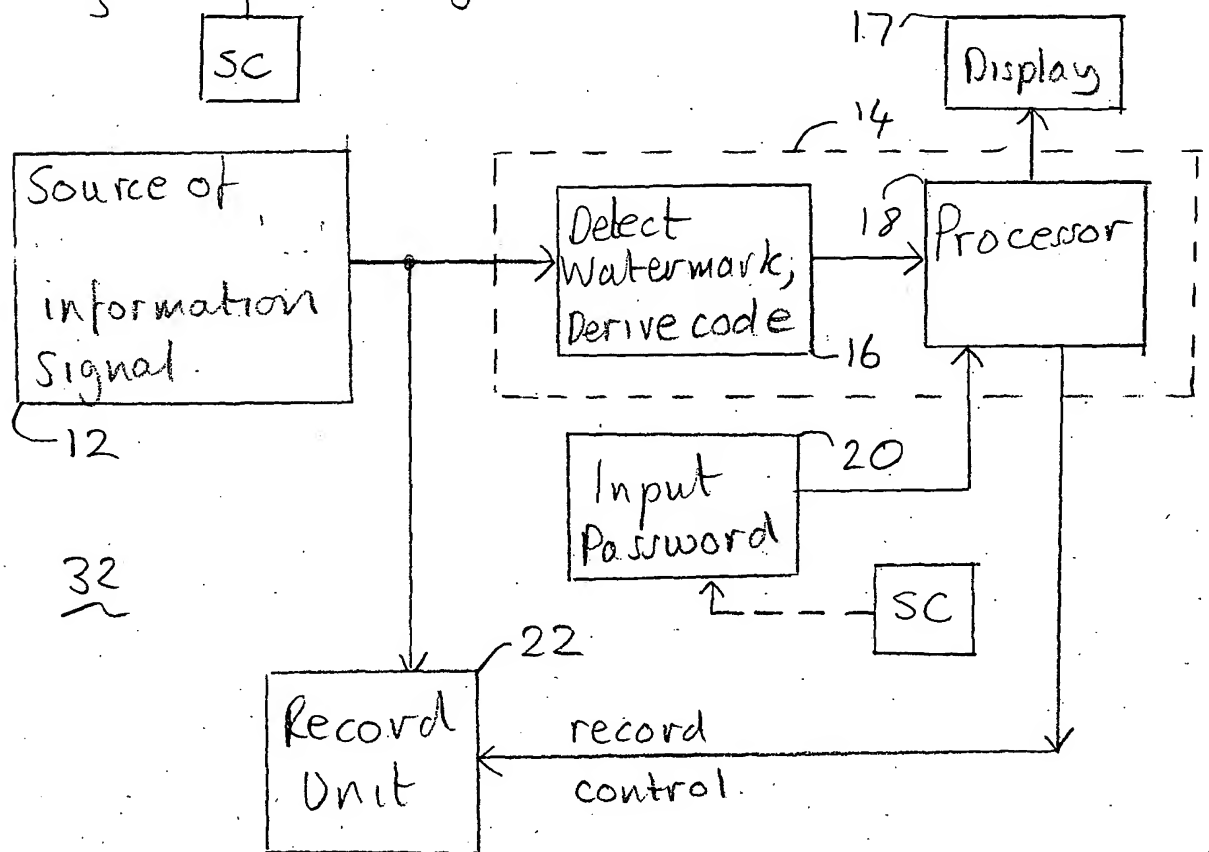
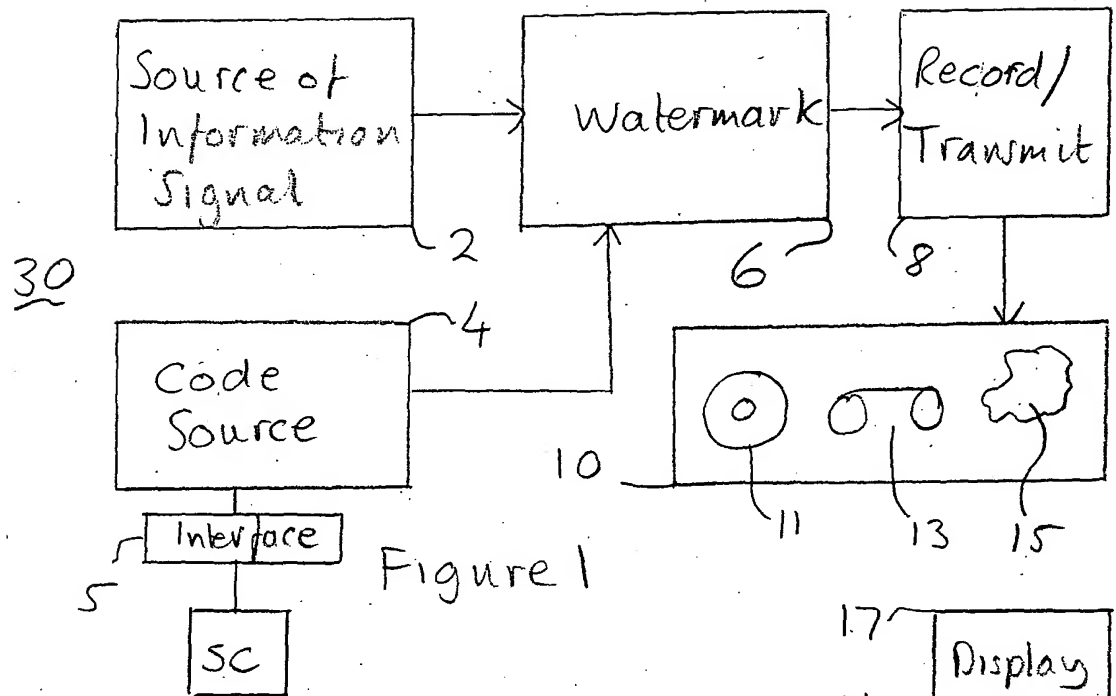
**ABSTRACT****Embedding Data in an Information Signal**

A method of controlling copying of an information signal, comprises the steps of:

- 5       prior to recordal and/or transmission, applying to the information signal a substantially imperceptible modification representing copy control data including a password securely encoded according to a predetermined algorithm;  
      upon reproduction for copying by a user, deriving (S1, S3) the copy control data from the modified information signal;
- 10       comparing (S8, S9, S11, S13, S15) the derived securely encoded password with a reference password securely encoded according to a predetermined algorithm; and  
      enabling (S5) copying of the information signal if the securely encoded password derived from the information signal and the securely encoded reference password have a predetermined relationship, otherwise disabling copying ( S7).
- 15       The reference password is sent to the user via a channel which is separate from a channel used to send the information signal to the user.

(Figure 3)

1/5



2/5

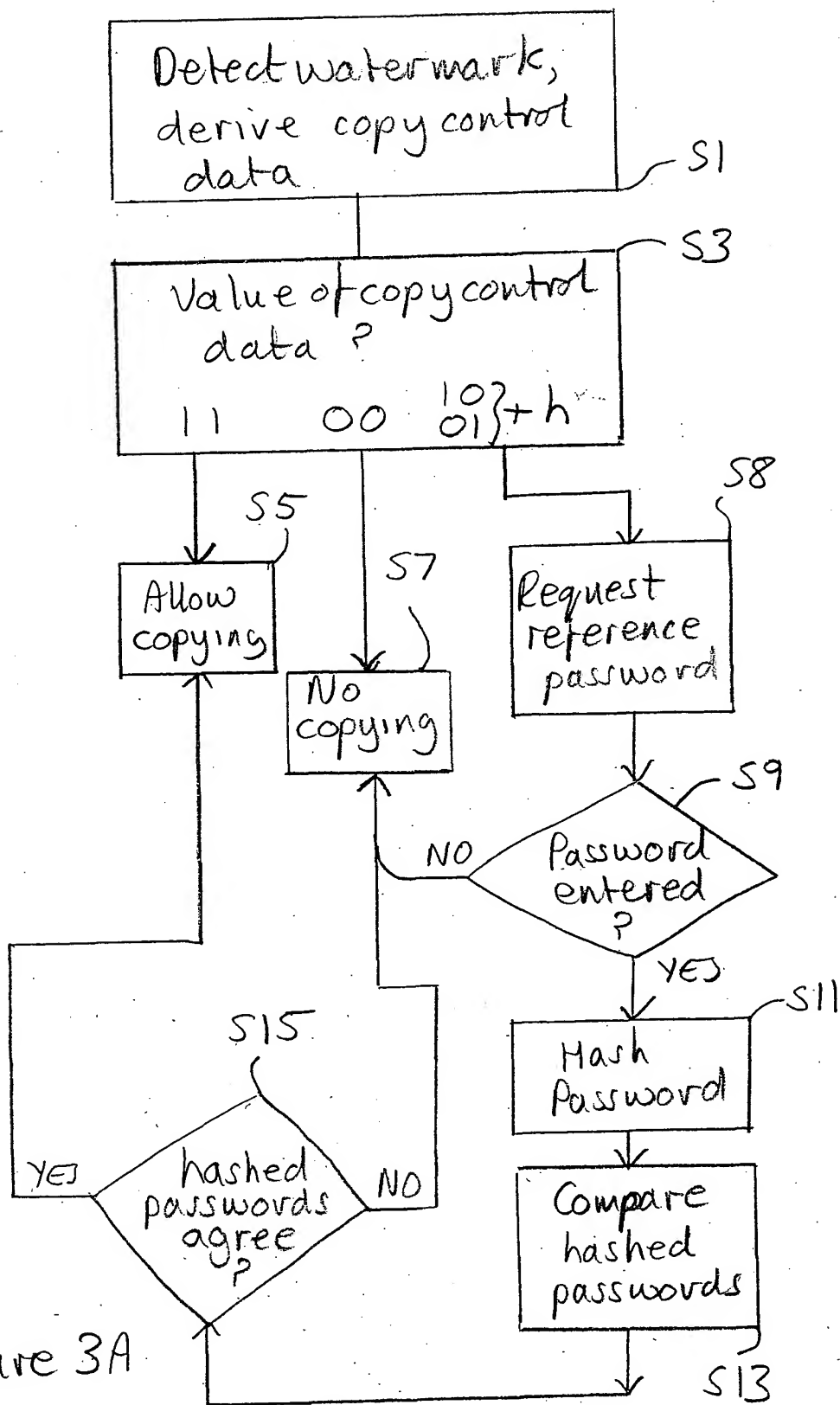


Figure 3A

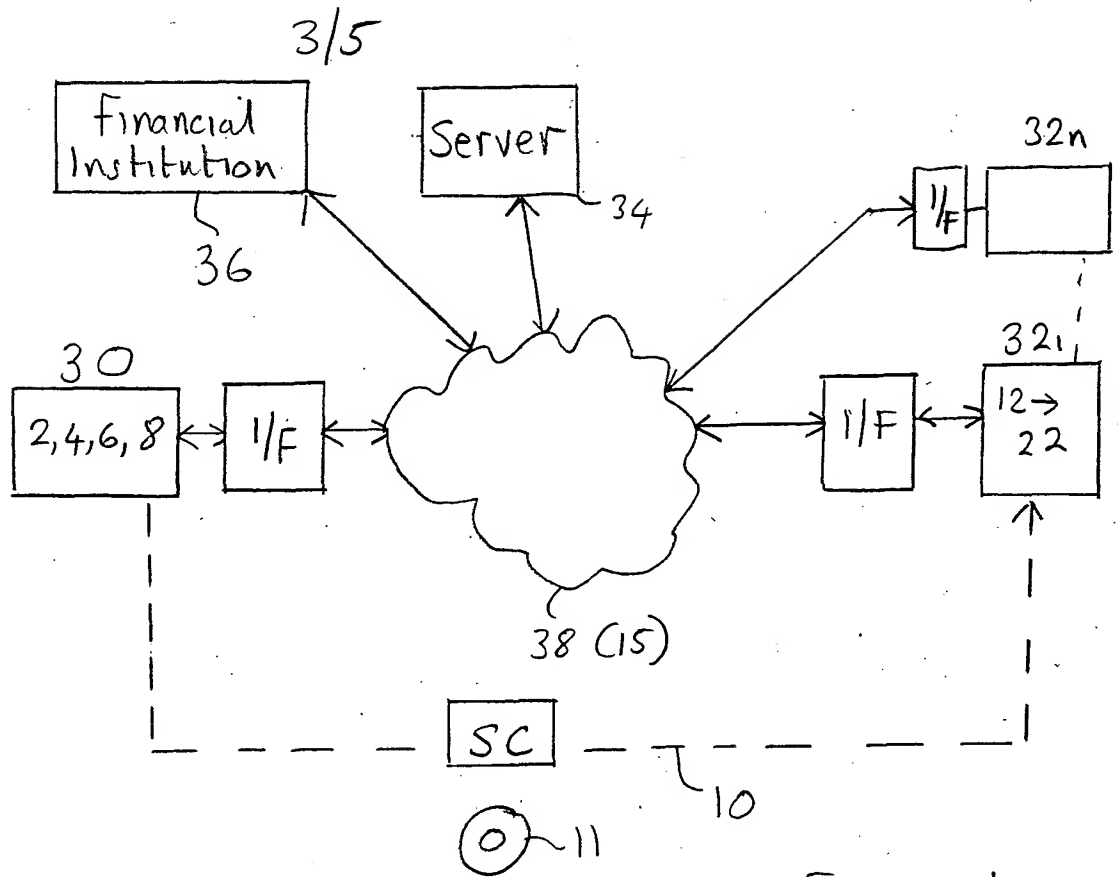


Figure 4.

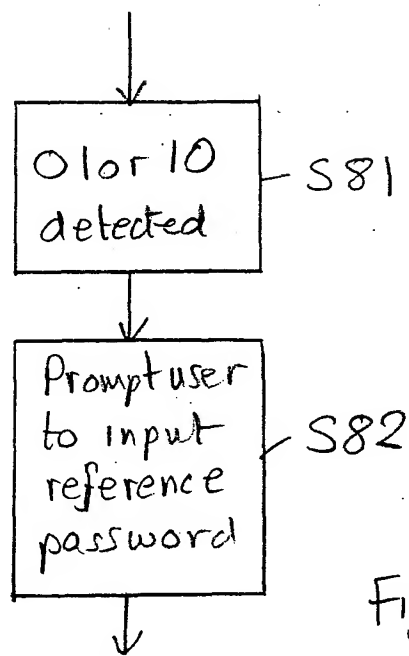


Figure 3B

4/5

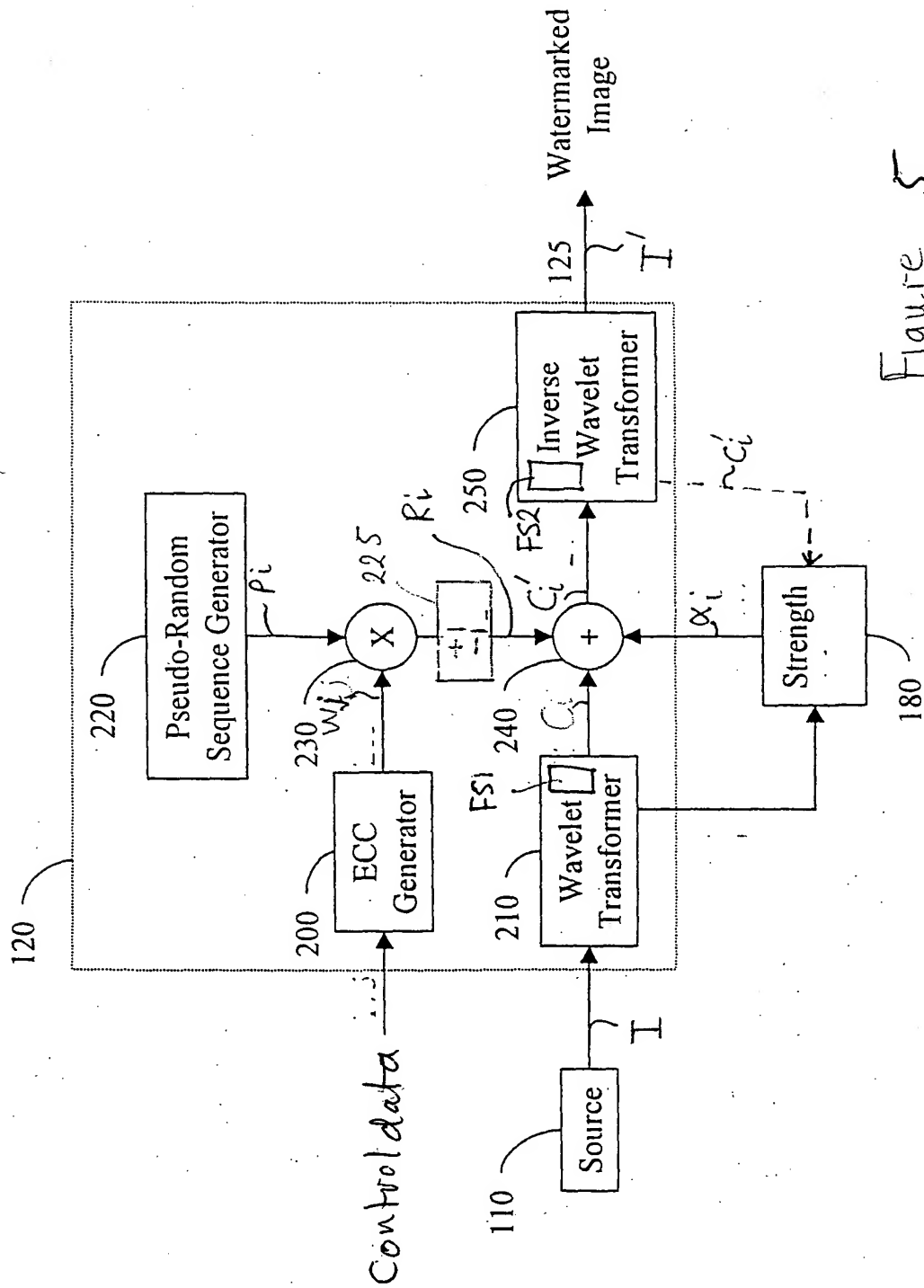


Figure 5

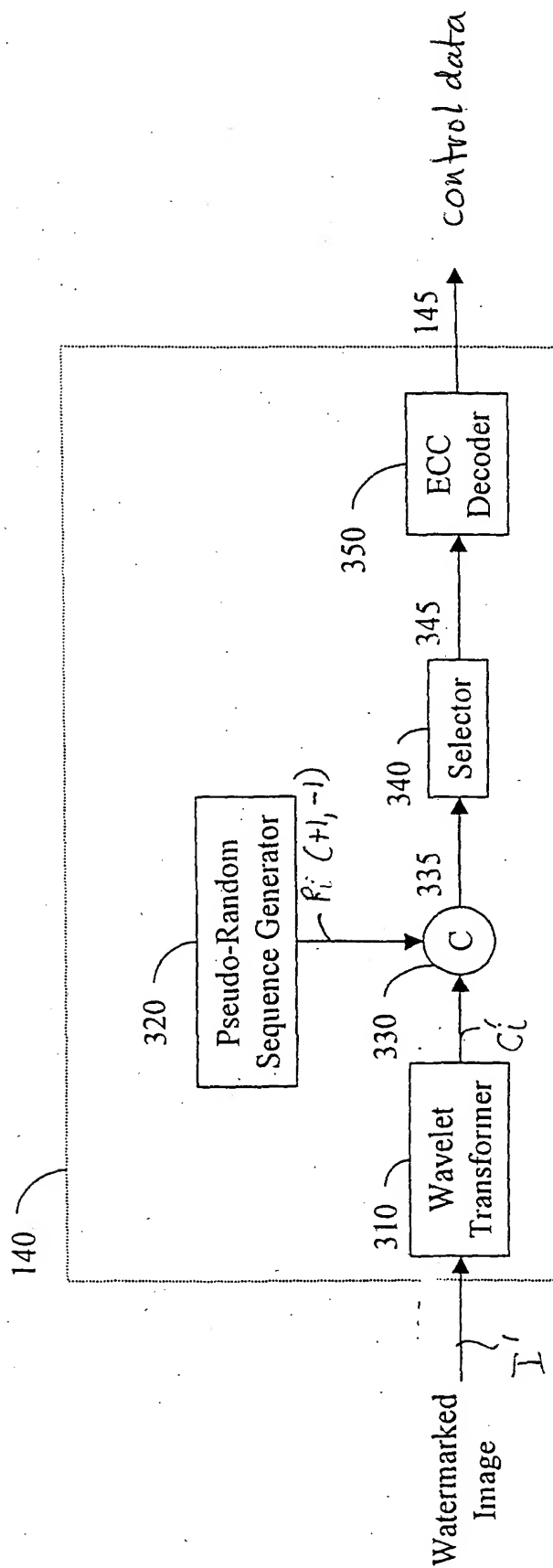


Figure 6